035014-1

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　３月３１日

出願番号
Application Number: 特願２００３－０９５６７１

[ST. 10/C]: ［ＪＰ２００３－０９５６７１］

出願人
Applicant(s): 株式会社東芝

２００３年　７月１８日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０５７５６７

【書類名】　特許願
【整理番号】　A000205954
【提出日】　平成15年 3月31日
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 15/00
【発明の名称】　オフライン情報を利用したデバイス認証装置及びデバイス認証方法
【請求項の数】　16
【発明者】
【住所又は居所】　東京都青梅市末広町２丁目９番地　株式会社東芝青梅事業所内
【氏名】　金澤　浩二
【発明者】
【住所又は居所】　東京都青梅市末広町２丁目９番地　株式会社東芝青梅事業所内
【氏名】　馬渡　正彦
【特許出願人】
【識別番号】　000003078
【氏名又は名称】　株式会社　東芝
【代理人】
【識別番号】　100058479
【弁理士】
【氏名又は名称】　鈴江　武彦
【電話番号】　03-3502-3181
【選任した代理人】
【識別番号】　100091351
【弁理士】
【氏名又は名称】　河野　哲

【選任した代理人】

【識別番号】　100088683

【弁理士】

【氏名又は名称】　中村　誠

【選任した代理人】

【識別番号】　100108855

【弁理士】

【氏名又は名称】　蔵田　昌俊

【選任した代理人】

【識別番号】　100084618

【弁理士】

【氏名又は名称】　村松　貞男

【選任した代理人】

【識別番号】　100092196

【弁理士】

【氏名又は名称】　橋本　良郎

【手数料の表示】

【予納台帳番号】　011567

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　オフライン情報を利用したデバイス認証装置及びデバイス認証方法

【特許請求の範囲】

【請求項１】　通信機能を持つ機器に設けられるデバイス認証装置であって、

他の機器によって可搬型の記録媒体に記録された認証データを読み込む読み込み手段と、

前記読み込み手段により読み込まれた前記認証データを記録する記録手段と、

前記記録手段に記録された前記認証データを用いて、前記他の機器との間で相互認証処理を行なう認証手段と

を具備したことを特徴とするデバイス認証装置。

【請求項２】　通信機能を持つ機器に設けられるデバイス認証装置であって、

認証データを生成する生成手段と、

前記生成手段により生成した前記認証データを可搬型の記録媒体に記録する認証データ記録手段と、

前記記録媒体に記録された前記認証データを記録する記録手段と、

前記記録手段により記録された前記認証データを用いて、前記可搬型の記録媒体から前記認証データを読み込んだ他の機器との間で相互認証処理を行なう認証手段と

を具備したことを特徴とするデバイス認証装置。

【請求項３】　前記記録手段は、

不揮発性の記録媒体によって前記認証データを記録することを特徴とする請求項１または請求項２記載のデバイス認証装置。

【請求項４】　前記認証手段は、

前記認証データに含まれる有効期間を示すデータをもとに、有効期間中にあるかを判別する判別手段と、

前記判別手段によって有効期間が経過したと判別された場合に、前記認証デー

タを無効にする無効手段とを具備したことを特徴とする請求項１記載のデバイス認証装置。

【請求項５】　前記生成手段は、

有効期間を示すデータを含む認証データを生成することを特徴とする請求項２記載のデバイス認証装置。

【請求項６】　前記認証手段は、

相互認証処理の実行回数を記憶する回数記憶手段と、

前記認証データに含まれる有効回数を示すデータをもとに、有効期間中にあるかを判別する判別手段と、

前記判別手段によって有効期間中にあると判別された場合に、前記認証データを無効にする無効手段とを具備したことを特徴とする請求項１記載のデバイス認証装置。

【請求項７】　前記生成手段は、

有効期間を示すデータを含む認証データを生成することを特徴とする請求項２記載のデバイス認証装置。

【請求項８】　前記認証手段は、

他の機器からの認証要求を受信する第１受信手段と、

前記第１受信手段に受信された認証要求に対して、前記認証データを用いて生成されるデータを前記他の機器に対して送信する第１送信手段と

を具備したことを特徴とする請求項１記載のデバイス認証装置。

【請求項９】　前記認証手段は、

前記他の機器に対して認証要求を送信する第２送信手段と、

前記第２送信手段によって送信した送信要求に応じて、前記他の機器から送信されるデータを受信する第２受信手段と、

前記第２受信手段によって受信したデータが前記認証データを用いて生成されているかを判別する判別手段と

を具備したことを特徴とする請求項２記載のデバイス認証装置。

【請求項１０】　前記認証手段は、

前記認証データを用いて生成されるデータを前記他の機器に対して送信する第

３送信手段と、

前記他の機器から送信されるデータを受信する第３受信手段と、

前記第３受信手段によって受信したデータが前記認証データを用いて生成されているかを判別する判別手段と

を具備したことを特徴とする請求項１または請求項２記載のデバイス認証装置。

【請求項１１】　前記可搬型の記録媒体は、記録されたデータの正当性が保証される記録媒体であることを特徴とする請求項１または請求項２記載のデバイス認証装置。

【請求項１２】　前記生成手段は、

所有者データを取得する取得手段と、

前記所有者データをもとに認証データを生成する認証データ生成手段と

を具備したことを特徴とする請求項２記載のデバイス認証装置。

【請求項１３】　前記取得手段は、

所有者の生体情報を入力する生体情報入力手段を有することを特徴とする請求項１３記載のデバイス認証装置。

【請求項１４】　前記取得手段は、

所有者データを入力する入力手段と、

前記入力手段によって入力された前記所有者データの正当性を確認する所有者データ確認手段とを有することを特徴とする請求項１３記載のデバイス認証装置。

【請求項１５】　通信機能を持つ機器におけるデバイス認証方法であって、

第１の機器において、認証データを生成して記録しておくと共に、可搬型の記録媒体に記録し、

第２の機器において、前記第１の機器によって可搬型の記録媒体に記録された認証データを前記可搬型の記憶媒体から読み込んで記録し、

前記第１の機器と前記第２機器の間で、それぞれに記憶された前記認証データを用いて相互認証処理を行なうことを特徴とするデバイス認証方法。

【請求項１６】　前記相互認証処理では、

前記第１の機器において前記認証データをもとに生成した第１のデータを前記

第２の機器に送信し、

前記第２の機器において前記認証データをもとに生成した第２のデータを前記第１の機器に送信し、

前記第１の機器において前記第２の機器から送信されたデータが前記認証データを用いて生成されているかを判別し、

前記第２の機器において前記第１の機器から送信されたデータが前記認証データを用いて生成されているかを判別する

ことを特徴とする請求項１５記載のデバイス認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、通信機能を有する機器におけるデバイス認証装置及びデバイス認証方法に関する。

【０００２】

【従来の技術】

従来、ライセンス技術を使用してライセンスされた限られた機器間で通信をする場合、例えばデジタルコンテンツを提供するサーバとコンテンツの提供先となるクライアント機器が通信をする場合には、クライアント機器がライセンスされた正しい機器であることを確認するために、通信を行なう前に認証処理を行っている。認証処理によってライセンスされた機器であることが確認されると、例えば暗号化されたコンテンツを解除するためのキー（データ）が交換され、クライアント機器においてコンテンツを扱うことができるようになる。

【０００３】

しかし、従来の認証処理では、通信相手の機器がライセンスされた技術を使用した正しい機器であるかどうかだけしか確認することはできない。このため、ライセンスされた機器の中でさらに限られた特定の機器のみを対象として通信することができない。

【０００４】

例えば、機器間が無線通信によって接続される場合、Ａ家内に設置された機器

にのみ通信を許可しようとしても、隣接しているＢ家に設置されているライセンスされた機器がＡ家の機器と無線通信が可能であれば、Ｂ家の機器においても何の制限も無く通信が可能となってしまう。従って、デジタルコンテンツの提供先として意図していない機器に対してもコンテンツが提供されてしまうことになる。

【０００５】

従来、ネットワークにログインする際に不正ログインを防止するために、ログイン情報を可搬の記録媒体に記録しておき、この記録媒体を用いてログインする方法が考えられている（例えば、特許文献１）。特許文献１のログイン方法では、ログイン情報（ユーザ情報）が記録された記録媒体を装着したクライアントＰＣのみがログインされネットワークを利用することができる。

【０００６】

【特許文献１】

特開２００２－２１５５９０号公報

【０００７】

【発明が解決しようとする課題】

このように従来では、機器間で認証処理を実行することで、ライセンス技術を使用してライセンスされた限られた機器のみを対象として接続相手とする機器を制限することができるが、ライセンスされた機器中でさらに限られた機器のみを通信相手として制限することができなかった。

【０００８】

本発明は前記のような事情を考慮してなされたもので、認証時に使用される認証データを可搬型の記憶媒体を通してオフラインで認証機器側から被認証機器側へ相互認証処理が行なわれる前に渡すことにより、ライセンスされた正しい機器のうち、事前に認証機器側からオフラインで認証データを取得した被認証機器だけを接続可能にするデバイス認証装置及びデバイス認証方法を提供することを目的とする。

【０００９】

【課題を解決するための手段】

本発明は、通信機能を持つ機器に設けられるデバイス認証装置であって、他の機器によって可搬型の記録媒体に記録された認証データを読み込む読み込み手段と、前記読み込み手段により読み込まれた前記認証データを記録する記録手段と、前記記録手段に記録された前記認証データを用いて、前記他の機器との間で相互認証処理を行なう認証手段とを具備したことを特徴とする。

【００１０】

また本発明は、通信機能を持つ機器に設けられるデバイス認証装置であって、認証データを生成する生成手段と、前記生成手段により生成した前記認証データを可搬型の記録媒体に記録する認証データ記録手段と、前記記録媒体に記録された前記認証データを記録する記録手段と、前記記録手段により記録された前記認証データを用いて、前記可搬型の記録媒体から前記認証データを読み込んだ他の機器との間で相互認証処理を行なう認証手段とを具備したことを特徴とする。

【００１１】

【発明の実施の形態】

以下、図面を参照して本発明の実施の形態について説明する。

本実施形態におけるデバイス認証装置は、例えば著作権保護機能等のライセンス技術を必要とする機器間の相互認証処理において、相互認証処理に必要とする認証データを可搬型のセキュアな記録媒体（ＳＤ（Secure digital）カード（登録商標）、メモリースティック（登録商標）等）を介してオフラインで提供し、このオフラインで提供された認証データを用いた相互認証処理を実行することで、機器がライセンス技術に準拠しているだけでなく、事前に認証データが提供された特定の機器だけが接続可能となるようにする。なお、本発明は、例えば著作権保護機能等のライセンス技術を必要とする機器間に限らず、ライセンス技術を必要としない機器間においても適用することができる。

【００１２】

図１は本実施形態に係わるデバイス認証装置１０、１２（１２ａ，１２ｂ，１２ｃ），１４の使用形態の一例を示す図である。本実施形態におけるデバイス認証装置１０、１２（１２ａ，１２ｂ，１２ｃ），１４は、例えば半導体メモリ、ＣＤ－ＲＯＭ、ＤＶＤ、磁気ディスク等の記録媒体に記録されたプログラムを読

み込み、このプログラムによって動作が制御されるコンピュータによって実現される。

【００１３】

図１において、デバイス認証装置１０は、例えばデジタルコンテンツを、ライセンスされた特定の他の機器に対して無線通信によって提供するサーバ（コンピュータ）によって実現される。以下、デバイスＡ１０（認証機器）として説明する。また、デバイス認証装置１２（１２ａ，１２ｂ，１２ｃ），１４は、デバイスＡ１０（サーバ）から提供されるデジタルコンテンツを受信するクライアント機器（コンピュータ）によって実現される。ただし、本実施形態において、デバイス認証装置１２（１２ａ，１２ｂ，１２ｃ），１４は、デバイスＡ１０との間の認証処理によりライセンスされた機器であることが確認されるだけでなく、可搬型の記憶媒体であるセキュアメモリカード１６を用いてオフラインで取得された認証データを用いた相互認証処理によって、デジタルコンテンツの利用が許可された特定の機器であることが確認される必要がある。

【００１４】

例えば、図１において、デバイスＡ１０は、相互認証処理に用いる認証データを生成してセキュアメモリカード１６に書き込む。例えば、建物Ｈ１内に設置されたクライアント機器１２ａ，１２ｂに対して、セキュアメモリカード１６を介して認証データを提供することで、クライアント機器１２ａ，１２ｂに対してコンテンツを利用させることができる。この場合、クライアント機器１２ｃは、セキュアメモリカード１６を介して認証データを取得していないので、建物Ｈ１に設置されていてもコンテンツを利用することができない。同様にして、建物Ｈ２内に設置されたクライアント機器１４は、デバイスＡ１０との間で無線通信が可能な範囲に設置されていても、セキュアメモリカード１６を介して認証データを取得していなければコンテンツを利用することができない。以下、デバイスＡ１０からセキュアメモリカード１６を介して認証データがされるクライアント機器１２ａ，１２ｂをデバイスＢ１２（被認証機器）として説明する。

【００１５】

図２は、図１に示すデバイスＡ１０とデバイスＢ１２の構成を示すブロック図

である。図２に示すように、デバイスＡ１０（サーバ）は、ＣＰＵ２０、ＲＯＭ２１、ＲＡＭ２２、カードスロット２３、記憶装置２４、ＥＥＰＲＯＭ（Electrically Erasable and Programmable ROM）２５、乱数発生部２６、通信ユニット２７、生体情報入力装置２８の他、図示していない表示装置（ＬＣＤ（Liquid Crystal Display）など）や入力装置（キーボード、マウスなど）等の一般的なコンピュータに設けられる機能を有している。

【００１６】

ＣＰＵ２０は、ＲＯＭ２１またはＲＡＭ２２に記録されたプログラムを実行することで各種の処理を実行するもので、例えばＲＯＭ２１に記録された認証プログラム３０により通信相手とする他の機器（デバイスＢ１２など）との相互認証を実行し、ライセンスされた機器であり、かつ予め通信が許可された機器であることを判別する。また、相互認証された他の機器に対して、記憶装置２４に記録されたデジタルコンテンツを提供するコンテンツサーバとして機能させる。ＣＰＵ２０は、認証プログラム３０を実行することによって、セキュアメモリカード１６に書き込んだ認証データを取得したデバイスＢ１２との間で、認証データを用いて相互認証処理を実行する。認証プログラム３０では、相互認証処理の対象とする他の機器（デバイスＢ１２）で実行される認証プログラム３２（後述する）と同じ関数に従う演算が可能である。

【００１７】

ＲＯＭ２１は、プログラムやデータが記録されるもので、他の機器の間で相互認証を行なう認証プログラム３０を含む。

【００１８】

ＲＡＭ２２は、プログラムやデータが記録される。

【００１９】

カードスロット２３は、可搬型の記録媒体に対してデータの読み込み／書き込みを実行する。カードスロット２３は、例えばＳＤカードなどの、記録されたデータの正当性が保証されるセキュアメモリカード１６を扱うものとする。

【００２０】

記憶装置２４は、プログラムやデータが記録される。デバイスＡ１０がデジタ

ルコンテンツのサーバとして使用される場合には、コンテンツデータが蓄積される。

【００２１】

ＥＥＰＲＯＭ２５は、不揮発性の記録媒体であり、例えば認証プログラム３０により生成された認証データが記録される。

【００２２】

乱数発生部２６は、他の機器（デバイスＢ１２）との間で相互認証処理を実行する際に必要となる乱数を生成する。

【００２３】

通信ユニット２７は、他の機器と通信を行なうもので、無線通信の他、ケーブルを介した通信を行なう。

【００２４】

生体情報入力装置２８は、生体情報（バイオメトリクス情報）を入力するもので、例えば指紋、掌紋、虹彩、網膜、掌などの静脈、声紋などのパターンデータを入力することができる。生体情報入力装置２８により入力された生体情報は、認証データの生成に用いられる所有者データとして扱われる（第２実施形態）。

【００２５】

デバイスＢ１２（クライアント）は、図２に示すように、ＣＰＵ２０、ＲＯＭ２１、ＲＡＭ２２、カードスロット２３、記憶装置２４、ＥＥＰＲＯＭ２５、乱数発生部２６、及び通信ユニット２７を有している。なお、デバイスＡ１０と同等の機能部分について同一符号を付して説明を省略する。

【００２６】

デバイスＢ１２のＲＯＭ２１には、デバイスＡ１０との間で相互認証をするための認証プログラム３２が記録されているものとする。ＣＰＵ２０は、認証プログラム３２を実行することによって、セキュアメモリカード１６から読み込んだ認証データを用いて、セキュアメモリカード１６に対して認証データを書き込んだデバイスＡ１０との間で相互認証処理を実行する。認証プログラム３２では、相互認証処理の対象とする他の機器（デバイスＡ１０）で実行される認証プログラム３０と同じ関数に従う演算が可能である。

【００２７】

なお、図２において、デバイスＡ１０とデバイスＢ１２のＲＯＭ２１に記録された認証プログラム３０，３２により認証処理を実行するものとして説明しているが、記憶装置２４に記録された認証プログラムをＲＡＭ２２にロードして実行されるとしても良い。記憶装置２４に記録された認証プログラムは、他の記録媒体（ＣＤ－ＲＯＭなど）か読み込まれて記録されても良いし、通信ユニット２７による通信によって受信して記録されても良い。

【００２８】

（第１実施形態）

次に、第１実施形態の動作について説明する。

図３は、デバイスＡ１０とデバイスＢ１２との間で行われる手続きのシーケンスを示す図、図４はデバイスＡ１０における相互認証処理の動作を説明するためのフローチャート、図５はデバイスＢ１２における相互認証処理の動作を説明するためのフローチャートである。デバイスＡ１０とデバイスＢ１２は、両方の機器ともに共通なライセンス技術を使用している。

【００２９】

まず、デバイスＡ１０は、認証を開始する前に、通信相手とする機器が正しいライセンス機器であるかどうかを判断するだけでなく、例えばデジタルコンテンツの利用を認めた機器であるかどうかを判断するために用いる認証データを生成する。すなわち、デバイスＡ１０は、認証プログラム３０を実行することで、乱数発生部２６において乱数（乱数Ｃとする）を生成させ（ステップＡ１）、この乱数Ｃをもとに他の機器との間で実行される相互認証処理に用いる認証データを生成し、ＥＥＰＲＯＭ２５に記録しておく（ステップＡ２）。なお、第１実施形態では、認証データは乱数Ｃのデータそのものとする。

【００３０】

デバイスＡ１０は、ＥＥＰＲＯＭ２５に記録した認証データを、カードスロット２３を通じてセキュアメモリカード１６に書き込む（ステップＡ３）。

【００３１】

デバイスＡ１０により生成された認証データ（乱数Ｃ）は、セキュアメモリカ

ード１６を介してオフラインでデバイスＢ１２、すなわち図１中に示す特定のクライアント機器１２ａ，１２ｂにのみ渡される（図３、Ｓ１１）。デバイスＢ１２は、カードスロット２３に装着されたセキュアメモリカード１６から、デバイスＡ１０において生成された認証データを読み込み、ＥＥＰＲＯＭ２５に記録しておく（図５、ステップＢ１）。

【００３２】

デバイスＡ１０において生成された認証データは、物理的な可搬型の記録媒体であるセキュアメモリカード１６を介してデバイスＢ１２に提供されるため、不特定の機器において取得されるおそれがない。また、セキュアメモリカード１６を用い手いるため記録された認証データの正当性が保証されている。また、１枚のセキュアメモリカード１６によって、コンテンツの利用を許可しようと意図する複数の機器に対して認証データを提供できる。また、デバイスＢ１２は、セキュアメモリカード１６から認証データを読み込んで記憶した後は、セキュアメモリカード１６をカードスロット２３に装着しておく必要はない。

【００３３】

こうして、デバイスＡ１０により生成された認証データがデバイスＢ１２に提供された後に、デバイスＡ１０とデバイスＢ１２との間で相互認証処理が実行可能となる。

【００３４】

認証を開始するデバイスＡ１０は、乱数発生部２６により乱数Ａの生成を行ない、通信相手であるデバイスＢ１２に対して通信ユニット２７から送信して（challenge－Ａ、Ｓ１２）認証要求をする（ステップＡ４）。

【００３５】

デバイスＢ１２は、デバイスＡ１０からのchallenge－Ａ、すなわち認証要求（乱数Ａ）を受信すると（ステップＢ２）、デバイスＡ１０から取得した乱数Ａを記録しておく。また、デバイスＢ１２は、challenge－Ａを送信してきた相手が正しい機器であるかどうかを確認するため、乱数発生部２６により乱数Ｂを生成して、challenge－Ａの送信デバイスであるデバイスＡ１０へ送信する（challenge－Ｂ、Ｓ１３）（ステップＢ３）。

【００３６】

デバイスＡ１０は、challenge－Ｂ（Ｓ１３）を受信すると（ステップＡ５）、challenge－Ｂで送信されてきた、デバイスＢ１２で生成された乱数Ｂを用いて、認証プログラム３０に従う関数Ｆを演算し（ステップＡ６）、この演算結果のデータをデバイスＢ１２へ送信する（response－Ｂ、Ｓ１４）（ステップＡ７）。

【００３７】

デバイスＢ１２は、デバイスＡ１０から送信されてきたresponse－Ｂを受信し（ステップＢ４）、デバイスＡ１０の確認を行なう（ステップＢ５）。すなわち、デバイスＢ１２は、デバイスＡ１０に送信した乱数Ｂを用いて、認証プログラム３２に従う関数Ｆを演算し、その演算結果とデバイスＡ１０から受信した演算結果が一致するかを判別する。ここで、演算結果が一致した場合に、デバイスＡ１０からの正しいresponse－Ｂであると確認する。

【００３８】

次に、デバイスＢ１２は、デバイスＡ１０からのchallenge－Ａが正しい認証要求であることが確認できたので、先にデバイスＡ１０から受信した乱数Ａの値と、セキュアメモリカード１６を介してオフラインにて取得した乱数Ｃを用いて関数Ｆを演算し（ステップＢ６）、演算結果をデバイスＡ１０へ送信する（response－Ａ、Ｓ１５）（ステップＢ７）。

【００３９】

デバイスＡ１０は、デバイスＢ１２から送信されてきたresponse－Ａを受信し（ステップＡ８）、デバイスＢ１２の確認を行なう（ステップＡ９）。すなわち、デバイスＡ１０は、デバイスＢ１２に送信した乱数Ａとセキュアメモリカード１６を介して提供した乱数Ｃ（ＥＥＰＲＯＭ２５に記録した認証データ）とを用いて、認証プログラム３０に従う関数Ｆを演算し、その演算結果とデバイスＢ１２から受信した演算結果が一致するかを判別する。ここで、演算結果が一致した場合に、デバイスＢ１２からの正しいresponse－Ａであると確認する。これにより、乱数ＡでデバイスＢ１２が正しいライセンス機器であることを確認でき、また乱数Ｃで更にデバイスＢ１２がデバイスＡ１０から事前に承認されたデバイス

であることを確認できる。

【００４０】

デバイスＡ１０において、正しいresponse－Ａであることが判断されると、認証されたデバイス間で有効なセッションキーを共有することが可能となる。従って、デバイスＢ１２は、例えばデバイスＡ１０から送信される暗号化されたデジタルコンテンツを、キーを用いて復号化して利用することができる。

【００４１】

このようにして、デバイスＡ１０により生成された認証データ（乱数Ｃ）がセキュアメモリカード１６を介してデバイスＢ１２に提供され、この認証データを用いてデバイスＡ１０とデバイスＢ１２との間で相互認証処理が実行される。従って、セキュアメモリカード１６から認証データを取得していないクライアント機器では、デバイスＡ１０と通信可能であり、またライセンスされた機器であったとしても、デバイスＡ１０により認証されない。このため、デバイスＡ１０から提供されるコンテンツを利用することができない。

【００４２】

（第２実施形態）

第１実施形態では、デバイスＡ１０において認証データを生成する場合、乱数発生部２６によって生成した乱数Ｃを用いているが、デバイスＡ１０を管理する例えば所有者に関するデータを用いて認証データを生成する。

【００４３】

第２実施形態では、図４に示すフローチャートのステップＡ１，Ａ２に代えてステップＡ１１，Ａ１２を実行する。

【００４４】

デバイスＡ１０は、他の機器との相互認証に用いる認証データを生成する場合、所有者に対して所有者データの入力を要求する。所有者データは、デバイスＡ１０の管理者個人を客観的に特定することが可能なデータであり、例えば管理者個人から取得されるバイオメトリクス情報（生体情報）や、第３者によって管理者個人に固有のものであることが保証される情報、例えばクレジットカード番号、銀行口座番号などの情報を用いることができる。

【００４５】

例えば、デバイスＡ１０は、認証データに生体情報を用いる場合、生体情報入力装置２８から生体情報（例えば指紋パターン）を入力し、この生体情報を所定の形式のデータに変換して認証データとする（ステップＡ１１，Ａ１２）。

【００４６】

なお、セキュアメモリカード１６を介してデバイスＢ１２に提供する認証データを生成する場合に、所有者データを用いる点以外は（ステップＡ１１，Ａ１２）、第１実施形態と同様の処理が実行されるものとして説明を省略する（ステップＡ３～Ａ９）。

【００４７】

図６には、デバイスＡ１０に入力される所有者データが、管理者個人に固有のものであることを第３者によって保証させるためのシステム構成を示している。

【００４８】

例えば、所有者データとしてクレジットカード番号を用いる場合、図６に示すように、デバイスＡ１０は、インターネットなどのネットワーク４０を介して、クレジット会社のサーバ４２と接続する。デバイスＡ１０は、認証データとして用いる所有者データ（クレジットカード番号）が入力された場合、ネットワーク４０を介してサーバ４２に問い合わせをする。サーバ４２への問い合わせでは、例えば、入力されたクレジットカード番号と、予めサーバ４２に登録されている管理者本人しか知り得ないＩＤやパスワード、氏名、住所などの個人データを管理者に入力させて送信する。サーバ４２は、個人データに対応づけて登録してあるクレジットカード番号と、デバイスＡ１０から初心したクレジットカード番号とを比較し、一致した場合に、管理者によって入力されたクレジットカード番号が正当であることをデバイスＡ１０に応答する。デバイスＡ１０は、サーバ４２によって入力されたクレジットカード番号が正当であることが保証された場合に、認証データとして用いて、セキュアメモリカード１６に書き込んで、他の機器に対して提供する。

【００４９】

このようにして、セキュアメモリカード１６を介してデバイスＢ１２に提供す

る認証データに、デバイスＡ１０の管理者個人を特定できる所有者データを用いることで、デバイスＡ１０の管理者によって不特定の機器に認証データが提供されることを防ぐことができる。すなわち、認証データを提供することは、管理者個人のデータを他者に提供することになるので、管理者がセキュアメモリカード１６を不特定の相手に渡したり、他者に無断で使用されることがないように慎重に扱うことが期待できる。このため、デバイスＡ１０の管理者が認めた特定の機器（デバイスＢ１２）においてのみ、デバイスＡ１０から提供されるコンテンツを利用させることができる。

【００５０】

なお、前述した説明では、所有者データをそのまま認証データとして用いるものとして説明しているが、入力された所有者データに所定の処理を施したデータに変換して用いることも可能である。

【００５１】

（第３実施形態）

第３実施形態では、デバイスＡ１０からデバイスＢ１２に対して提供する認証データに、認証データの有効期間を示す有効期間回数データを含める。図７（ａ）には、デバイスＡ１０においてセキュアメモリカード１６に記録される認証データを示している。

【００５２】

デバイスＡ１０は、所有者データを生成する場合、第１実施形態のように乱数Ｃを生成する、あるいは第２実施形態のように所有者データを入力する（ステップＡ１、Ａ１１）。以下の説明では、乱数Ｃを用いるものとして説明する。

【００５３】

また、デバイスＡ１０は、有効期間データを生成し、この有効期間データと乱数Ｃまたは所有者データによって認証データを生成し（図７（ａ））（ステップＡ２、Ａ１２）、セキュアメモリカード１６に書き込む。有効期間データは、デバイスＡ１０の管理者によって入力装置から入力された有効期間に応じて生成されても良いし、認証プログラム３０において予め決められていても良い。有効期間データによって、認証データの有効期間を、例えば１週間、１カ月のように指

定することができる。また、有効期間は、デバイスＡ１０において認証データが生成されてからの期間に対するものでも良いし、デバイスＢ１２においてセキュアメモリカード１６から読み込まれて記憶されてからの期間に対するものでも良い。

【００５４】

図８はデバイスＢ１２における相互認証処理の動作を説明するためのフローチャートである。

【００５５】

デバイスＡ１０により生成された認証データは、セキュアメモリカード１６を介してオフラインでデバイスＢ１２、すなわち図１中に示す特定のクライアント機器１２ａ，１２ｂにのみ渡される。デバイスＢ１２は、カードスロット２３に装着されたセキュアメモリカード１６から、デバイスＡ１０において生成された認証データを読み込み、ＥＥＰＲＯＭ２５に記録しておく（図８、ステップＣ１）。また、デバイスＢ１２は、セキュアメモリカード１６から読み込んだ、認証データに対する有効期間データをＥＥＰＲＯＭ２５に記録しておく（ステップＣ２）。

【００５６】

なお、図８に示すステップＣ３～Ｃ６の処理については、図５のフローチャートに示すステップＢ２～Ｂ５の処理と同様にして実行されるものとして説明を省略する。

【００５７】

デバイスＢ１２は、ステップＣ６の処理によって、デバイスＡ１０が確認されると、現在、認証データの有効期間内にあるかを、ＥＥＰＲＯＭ２５に記録した有効期間データをもとに確認する（ステップＣ７）。

【００５８】

ここで、有効期間内であると確認できた場合、デバイスＢ１２は、先にデバイスＡ１０から受信した乱数Ａの値と、セキュアメモリカード１６を介してオフラインにて取得した乱数Ｃを用いて関数Ｆを演算し（ステップＣ９）、演算結果をデバイスＡ１０へ送信する（ステップＣ１０）（図５、ステップＢ６，Ｂ７と同

じ）。

【００５９】

一方、有効期間内にないと確認できた場合、デバイスＢ１２は、先にデバイスＡ１０から受信した乱数Ａの値を用いて関数Ｆを演算し（ステップＣ１１）、演算結果をデバイスＡ１０へ送信する（ステップＣ１０）。すなわち、セキュアメモリカード１６を介して取得した認証データを用いないで認証処理を実行する。この場合の認証処理では、ライセンスされた機器であることが確認することができる。

【００６０】

なお、有効期間内にないと確認できた場合には、認証が失敗したものと扱うようにしても良い。

【００６１】

このようにして、認証データに有効期間データを含めることで、デバイスＡ１０から提供するコンテンツを他の機器（デバイスＢ１２）が期限無く使用できることを防ぎ、またコンテンツを使用できる機器が制限無く増加することを防止できる。

【００６２】

（第４実施形態）

第４実施形態では、デバイスＡ１０からデバイスＢ１２に対して提供する認証データに、認証データを用いた認証処理の有効実行回数を示す有効使用回数データを含める。図７（ｂ）には、デバイスＡ１０においてセキュアメモリカード１６に記録される認証データを示している。

【００６３】

デバイスＡ１０は、所有者データを生成する場合、第１実施形態のように乱数Ｃを生成する、あるいは第２実施形態のように所有者データを入力する（ステップＡ１、Ａ１１）。以下の説明では、乱数Ｃを用いるものとして説明する。

【００６４】

また、デバイスＡ１０は、有効使用回数データを生成し、この有効使用回数データと乱数Ｃまたは所有者データによって認証データを生成し（図７（ｂ））（

ステップＡ２、Ａ１２）、セキュアメモリカード１６に書き込む。有効使用回数データは、デバイスＡ１０の管理者によって入力装置から入力された有効使用回数に応じて生成されても良いし、認証プログラム３０において予め決められていても良い。有効使用回数データによって、認証データの有効使用回数を、例えば１０回、１００回のように指定することができる。

【００６５】

図９はデバイスＢ１２における相互認証処理の動作を説明するためのフローチャートである。

【００６６】

デバイスＡ１０により生成された認証データは、セキュアメモリカード１６を介してオフラインでデバイスＢ１２、すなわち図１中に示す特定のクライアント機器１２ａ，１２ｂにのみ渡される。デバイスＢ１２は、カードスロット２３に装着されたセキュアメモリカード１６から、デバイスＡ１０において生成された認証データを読み込み、ＥＥＰＲＯＭ２５に記録しておく（図９、ステップＤ１）。また、デバイスＢ１２は、セキュアメモリカード１６から読み込んだ、認証データに対する有効使用回数データをＥＥＰＲＯＭ２５に記録しておく（ステップＤ２）。

【００６７】

なお、図８に示すステップＤ３～Ｄ６の処理については、図５のフローチャートに示すステップＢ２～Ｂ５の処理と同様にして実行されるものとして説明を省略する。

【００６８】

デバイスＢ１２は、ステップＤ６の処理によって、デバイスＡ１０が確認されると、現在、認証データを用いた認証処理の実行回数が有効使用回数内にあるかを、ＥＥＰＲＯＭ２５に記録した有効使用回数データをもとに確認する（ステップＣ７）。なお、認証データを用いた認証処理の実行回数（認証データの使用回数）は、認証データを用いた演算処理を実行する毎にカウントしている（後述するステップＤ１０）。

【００６９】

ここで、有効使用回数内であると確認できた場合、デバイスＢ１２は、先にデバイスＡ１０から受信した乱数Ａの値と、セキュアメモリカード１６を介してオフラインにて取得した乱数Ｃを用いて関数Ｆを演算し（ステップＤ９）、認証データの使用回数に１を加算して記憶し（ステップＤ１０）、演算結果をデバイスＡ１０へ送信する（ステップＤ１１）。

【００７０】

一方、有効使用回数内にないと確認できた場合、デバイスＢ１２は、先にデバイスＡ１０から受信した乱数Ａの値を用いて関数Ｆを演算し（ステップＤ１２）、演算結果をデバイスＡ１０へ送信する（ステップＤ１１）。すなわち、セキュアメモリカード１６を介して取得した認証データを用いないで認証処理を実行する。この場合の認証処理では、ライセンスされた機器であることが確認することができる。

【００７１】

なお、有効使用回数内にないと確認できた場合には、認証が失敗したものと扱うようにしても良い。

【００７２】

このようにして、認証データに有効使用回数データを含めることで、デバイスＡ１０から提供するコンテンツを他の機器（デバイスＢ１２）が無制限に使用できることを防ぐことができる。

【００７３】

なお、第３実施形態と第４実施形態の説明では、それぞれ有効期間データあるいは有効使用回数データの何れかを用いるものとしているが、両方を認証データに含めてセキュアメモリカード１６に書き込んで、他の機器に対して提供するようにしても良い。セキュアメモリカード１６を介してオフラインで認証データを取得した機器では、前述した説明のようにして、有効期間データと有効使用回数データの両方を用いて認証データの使用制限を管理する。

【００７４】

また、第３実施形態と第４実施形態の説明では、デバイスＡ１０において生成された認証データを取得したデバイスＢ１２において、有効使用回数を越えた場

合、あるいは有効期間を越えた場合には、認証データを用いた相互認証を行わないものとして説明しているが、認証データを生成したデバイスＡ１０側で有効使用回数、あるいは有効期間を確認するようにしても良い。この場合、デバイスＡ１０は、有効使用回数あるいは有効期間を越えたことが確認できた場合に、認証データを用いた相互認証を行わない。

【００７５】

（第５実施形態）

前述した第１～第４実施形態では、デバイスＢ１２からデバイスＡ１０に対して、乱数Ｃを用いて算出された関数Ｆの演算結果を送信しているが（ステップＢ６～Ｂ７、Ｃ９～Ｃ１０、Ｄ９～Ｄ１１）、デバイスＡ１０からデバイスＢ１２に対しても乱数Ｃを用いて算出された関数Ｆの演算結果を送信することで、相互認証をより確実にする。

【００７６】

図１０は、第５実施形態におけるデバイスＡ１０とデバイスＢ１２との間で行われる手続きのシーケンスを示す図である。なお、図１０に示すＳ２３，Ｓ２４に関係する処理以外（図３中に示すＳ１３，Ｓ１４に対応する）は、図３に示す処理と同様にして実行されるものとして説明を省略する。

【００７７】

デバイスＢ１２は、デバイスＡ１０からのchallenge－Ａ、すなわち認証要求（乱数Ａ）を受信すると、デバイスＡ１０から取得した乱数Ａを記録しておく。また、デバイスＢ１２は、challenge－Ａを送信してきた相手が正しい機器であるかどうかを確認するため、乱数発生部２６により乱数Ｂを生成し、この乱数Ａとセキュアメモリカード１６を介して取得した認証データ（乱数Ｃ）とを、challenge－Ａの送信デバイスであるデバイスＡ１０へ送信する（challenge－Ｂ、Ｓ２３）。

【００７８】

デバイスＡ１０は、challenge－Ｂ（Ｓ２３）を受信すると、challenge－Ｂで送信されてきた、デバイスＢ１２で生成された乱数Ｂと、ＥＥＰＲＯＭ２５に記憶してある他の機器に対してセキュアメモリカード１６を介して提供した認証デ

ータ（乱数Ｃ）を用いて、認証プログラム３０に従う関数Ｆを演算し、この演算結果のデータをデバイスＢ１２へ送信する（response－Ｂ、Ｓ２４）。

【００７９】

デバイスＢ１２は、デバイスＡ１０から送信されてきたresponse－Ｂを受信し、デバイスＡ１０の確認を行なう。すなわち、デバイスＢ１２は、デバイスＡ１０に送信した乱数Ｂとセキュアメモリカード１６を介して取得した認証データ（乱数Ｃ）を用いて、認証プログラム３２に従う関数Ｆを演算し、その演算結果とデバイスＡ１０から受信した演算結果が一致するかを判別する。ここで、演算結果が一致した場合に、デバイスＡ１０からの正しいresponse－Ｂであると確認する。

【００８０】

このようにして、第１～第４実施形態のように、デバイスＢ１２からデバイスＡ１０に対して、乱数Ｃを用いて算出された関数Ｆの演算結果を送信するだけでなく、デバイスＡ１０からデバイスＢ１２に対しても、他の機器に提供した認証データ（乱数Ｃ）を用いて算出された関数Ｆの演算結果を送信することで、相互認証をより確実にすることができる。

【００８１】

（第６実施形態）

第１～第５各実施形態では、デバイスＡ１０側からデバイスＢ１２に対して認証要求を行っているが（challenge－Ａ）、デバイスＢ１２からデバイスＢ１２に対して認証要求を行なうようにしても良い。

【００８２】

図１１は、第６実施形態におけるデバイスＡ１０とデバイスＢ１２との間で行われる手続きのシーケンスを示す図である。

【００８３】

この場合、デバイスＡ１０において生成される認証データを、セキュアメモリカード１６を介して他のデバイスＢ１２に提供する処理については、第１実施形態（Ｓ１１）と同様にして行われる物とする（Ｓ３１）。

【００８４】

デバイスＡ１０により生成された認証データがデバイスＢ１２に提供された後に、デバイスＡ１０とデバイスＢ１２との間で相互認証処理が実行可能となる。

【００８５】

認証を開始するデバイスＢ１２は、乱数発生部２６により乱数Ｂの生成を行ない、通信相手であるデバイスＡ１０に対して通信ユニット２７から送信して（challenge－Ｂ、Ｓ３２）認証要求をする。

【００８６】

デバイスＡ１０は、デバイスＢ１２からのchallenge－Ｂ、すなわち認証要求（乱数Ｂ）を受信すると、デバイスＢ１２から取得した乱数Ｂを記録しておく。また、デバイスＡ１０は、challenge－Ｂを送信してきた相手が正しい機器であるかどうかを確認するため、乱数発生部２６により乱数Ａを生成して、challenge－Ｂの送信デバイスであるデバイスＢ１２へ送信する（challenge－Ａ、Ｓ３３）。

【００８７】

デバイスＢ１２は、challenge－Ａ（Ｓ３３）を受信すると、challenge－Ａで送信されてきた、デバイスＡ１０で生成された乱数Ａとセキュアメモリカード１６を介して取得した認証データ（乱数Ｃ）を用いて、認証プログラム３２に従う関数Ｆを演算し、この演算結果のデータをデバイスＡ１０へ送信する（response－Ａ、Ｓ３４）。

【００８８】

デバイスＡ１０は、デバイスＢ１２から送信されてきたresponse－Ａを受信し、デバイスＢ１２の確認を行なう。すなわち、デバイスＡ１０は、デバイスＢ１２に送信した乱数Ａと、セキュアメモリカード１６を介して他の機器に提供した認証データ（乱数Ｃ）を用いて、認証プログラム３２に従う関数Ｆを演算し、その演算結果とデバイスＢ１２から受信した演算結果が一致するかを判別する。ここで、演算結果が一致した場合に、デバイスＢ１２からの正しいresponse－Ａであると確認する。

【００８９】

次に、デバイスＡ１０は、デバイスＢ１２からのchallenge－Ａが正しい認証

要求であることが確認できたので、先にデバイスＢ１２から受信した乱数Ｂの値（あるいは乱数Ｂの値とセキュアメモリカード１６を介して提供した乱数Ｃ）を用いて関数Ｆを演算し、演算結果をデバイスＢ１２へ送信する（response－Ｂ、Ｓ３５）。

【００９０】

デバイスＢ１２は、デバイスＡ１０から送信されてきたresponse－Ｂを受信し、デバイスＡ１０の確認を行なう。すなわち、デバイスＢ１２は、デバイスＡ１０に送信した乱数Ｂ（あるいは乱数Ｂとセキュアメモリカード１６を介して取得した乱数Ｃ）とを用いて、認証プログラム３２に従う関数Ｆを演算し、その演算結果とデバイスＡ１０から受信した演算結果が一致するかを判別する。ここで、演算結果が一致した場合に、デバイスＡ１０からの正しいresponse－Ｂであると確認する。これにより、乱数Ｂでデバイスａ１０が正しいライセンス機器であることを確認でき、また乱数Ｃで更に故知の提供元であるデバイスＡ１０であることを確認できる。

【００９１】

デバイスＢ１２において、正しいresponse－Ｂであることが判断されると、認証されたデバイス間で有効なセッションキーを共有することが可能となる。従って、デバイスＢ１２は、例えばデバイスＡ１０から送信される暗号化されたデジタルコンテンツを、キーを用いて復号化して利用することができる。

【００９２】

このようにして、デバイスＡ１０からセキュアメモリカード１６を介して認証データが提供されたデバイスＢ１２側から、デバイスＡ１０に対して認証要求を行って相互認証処理を実行することができる。第６実施形態におけるシーケンスを、第２～第５実施形態に適用することも可能である。

【００９３】

なお、前述した各実施形態の説明では、デバイスＢ１２は、１つのデバイスＡ１０からの認証データ（乱数Ｃ）を、セキュアメモリカード１６を介して取得するとしているが、複数のデバイスからそれぞれにおいて生成された認証データを、同様にしてセキュアメモリカードから読み出して記憶しておくこともできる。

この場合、デバイスＢ１２は、他のデバイスから認証要求があった場合に、複数の認証データから１つを選択して他のデバイスとの間で認証処理を実行する。そして、この認証データを用いて認証に失敗した際に、次の認証データを選択して同様に認証処理を実行する。この処理を認証が成立するまで繰り返して実行する。これにより、デバイスＢは、複数の異なるデバイスとの間で、それぞれ異なる認証データを用いて相互認証をすることができる。

【００９４】

また、デバイス認証装置１０は、コンピュータによって実現されるものとしているが、スタンドアロンタイプの単体の装置として構成することも可能である。この場合、コンピュータに接続されて使用され、コンピュータからの要求に応じて認証処理処理を実行する。

【００９５】

このようにして、著作権保護機能等のライセンスを必要とする機器間の認証処理においては、ライセンスを持った正しい機器であることを認証するだけでなく、可搬型の記憶媒体（セキュアメモリカード１６）を用いてオフラインで認証データを取得している機器を認証して、通信相手の制限を行うことが可能となる。

【００９６】

なお、上述した実施形態において記載した手法は、コンピュータに実行させることのできるプログラムとして、例えば磁気ディスク（フレキシブルディスク、ハードディスク等）、光ディスク（ＣＤ－ＲＯＭ、ＤＶＤ等）、半導体メモリなどの記録媒体に書き込んで各種装置に提供することができる。また、通信媒体により伝送して各種装置に提供することも可能である。本装置を実現するコンピュータは、記録媒体に記録されたプログラムを読み込み、または通信媒体を介してプログラムを受信し、このプログラムによって動作が制御されることにより、上述した処理を実行する。

【００９７】

また、本願発明は、前述した実施形態に限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で種々に変形することが可能である。更に、前記実施形態には種々の段階の発明が含まれており、開示される複数の構成要件におけ

る適宜な組み合わせにより種々の発明が抽出され得る。例えば、実施形態に示される全構成要件から幾つかの構成要件が削除されても効果が得られる場合には、この構成要件が削除された構成が発明として抽出され得る。

【００９８】

【発明の効果】

以上詳述したように本発明によれば、認証時に使用される認証データを可搬型の記憶媒体を通してオフラインで認証機器側から被認証機器側へ相互認証処理が行なわれる前に渡すことにより、この認証データを用いて機器間で相互認証処理が実行されるので、ライセンスされた正しい機器のうち、事前に認証機器側からオフラインで認証データを取得した被認証機器だけを接続可能にすることが可能となる。

【図面の簡単な説明】

【図１】　本実施形態に係わるデバイス認証装置１０、１２，１４の使用形態の一例を示す図。

【図２】　図１に示すデバイスＡ１０とデバイスＢ１２の構成を示すブロック図。

【図３】　デバイスＡ１０とデバイスＢ１２との間で行われる手続きのシーケンスを示す図。

【図４】　デバイスＡ１０における相互認証処理の動作を説明するためのフローチャート。

【図５】　デバイスＢ１２における相互認証処理の動作を説明するためのフローチャート。

【図６】　デバイスＡ１０に入力される所有者データが管理者個人に固有のものであることを第３者によって保証させるためのシステム構成を示す図。

【図７】　有効期間回数データまたは有効期間データを含む認証データの構成例を示す図。

【図８】　デバイスＢ１２における相互認証処理の動作を説明するためのフローチャート。

【図９】　デバイスＢ１２における相互認証処理の動作を説明するためのフ

ローチャート。

【図１０】　デバイスＡ１０とデバイスＢ１２との間で行われる手続きのシーケンスを示す図。

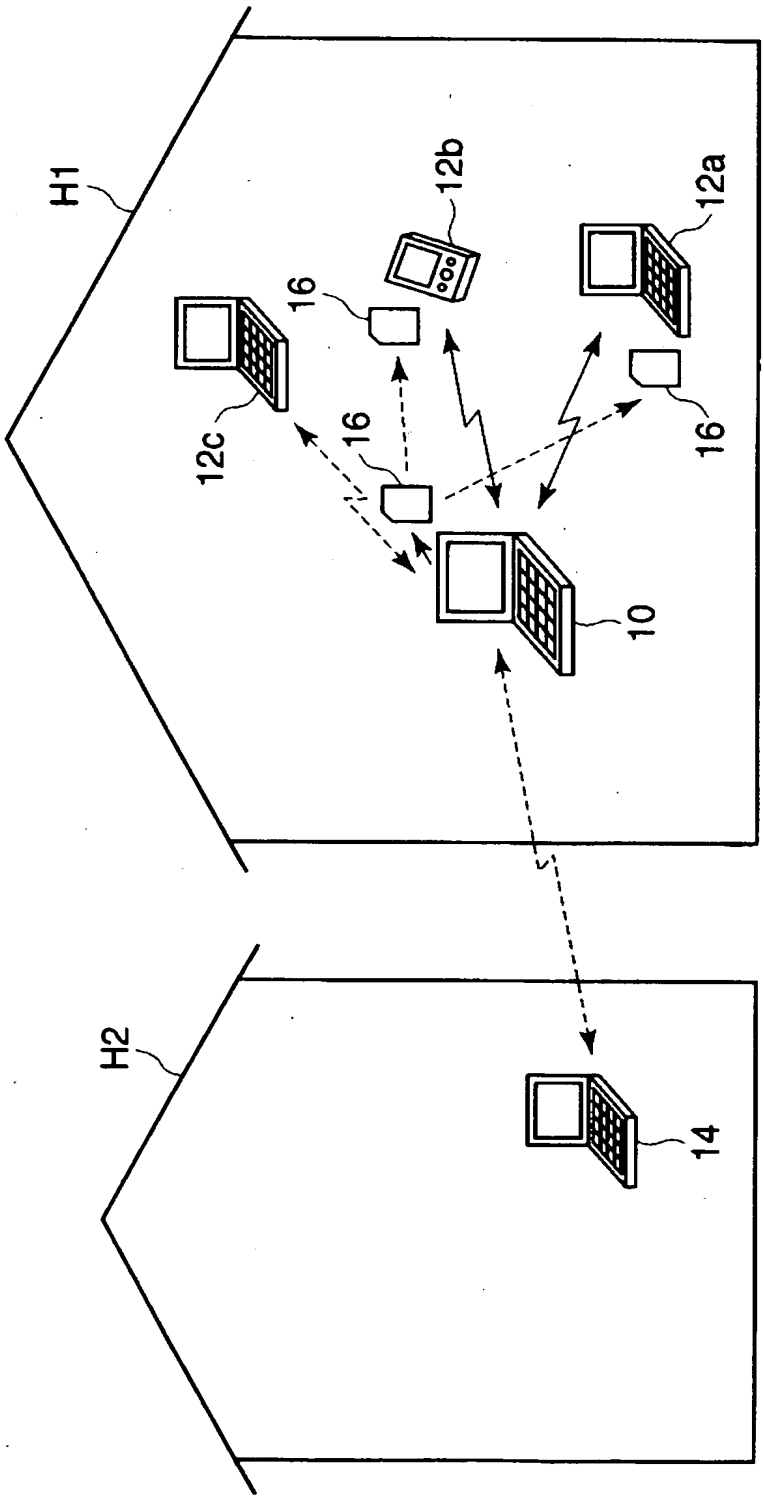
【図１１】　デバイスＡ１０とデバイスＢ１２との間で行われる手続きのシーケンスを示す図。

【符号の説明】

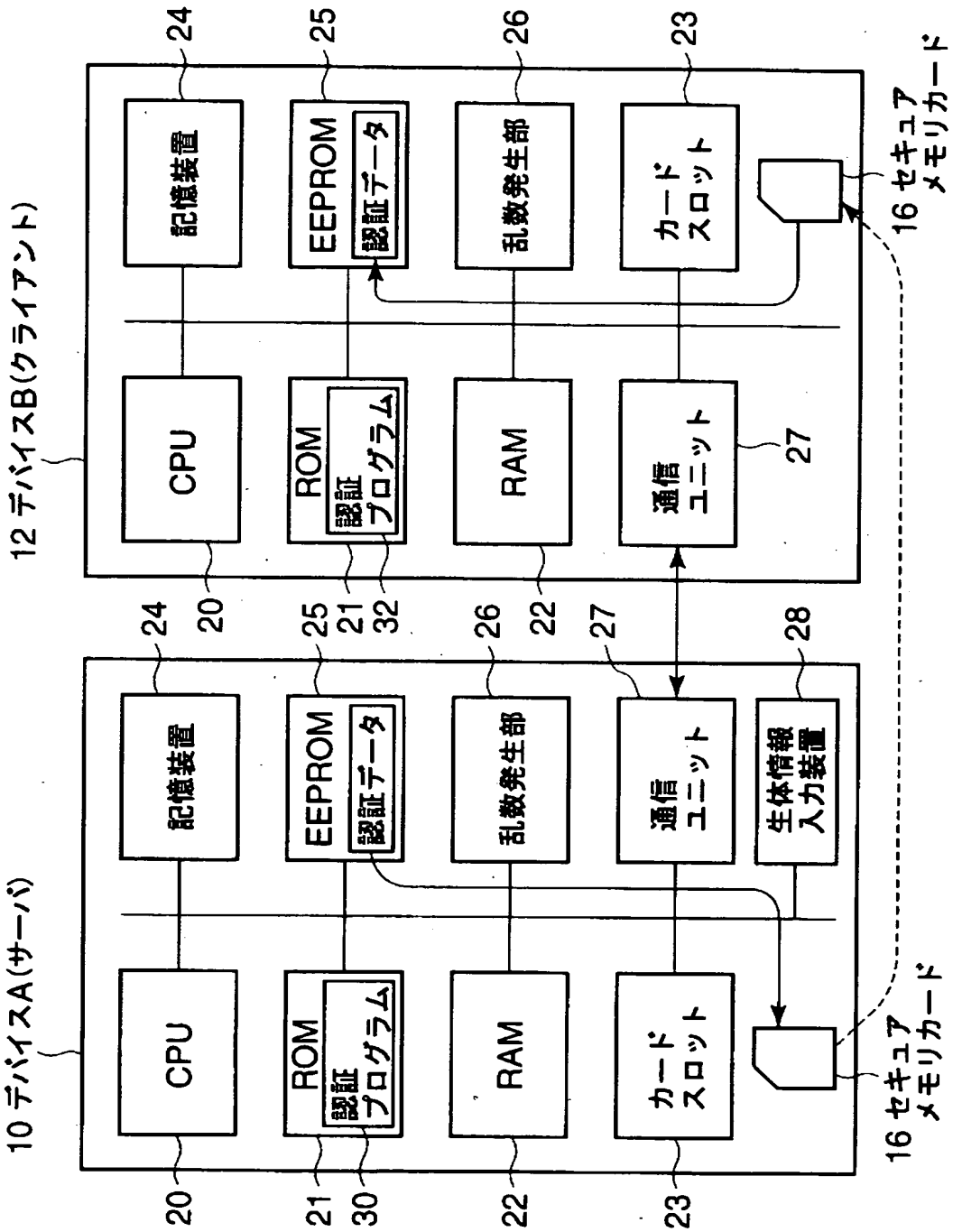
１０…デバイスＡ、１２（１２ａ，１２ｂ，１２ｃ）…デバイスＢ、１４…デバイス、１６…セキュアメモリカード、２０…ＣＰＵ、２１…ＲＯＭ、２２…ＲＡＭ、２３…カードスロット、２４…記憶装置、２５…ＥＥＰＲＯＭ、２６…乱数発生部、２７…通信ユニット、２８…生体情報入力装置、４０…ネットワーク、４２…所有者情報認証装置。

【書類名】　図面

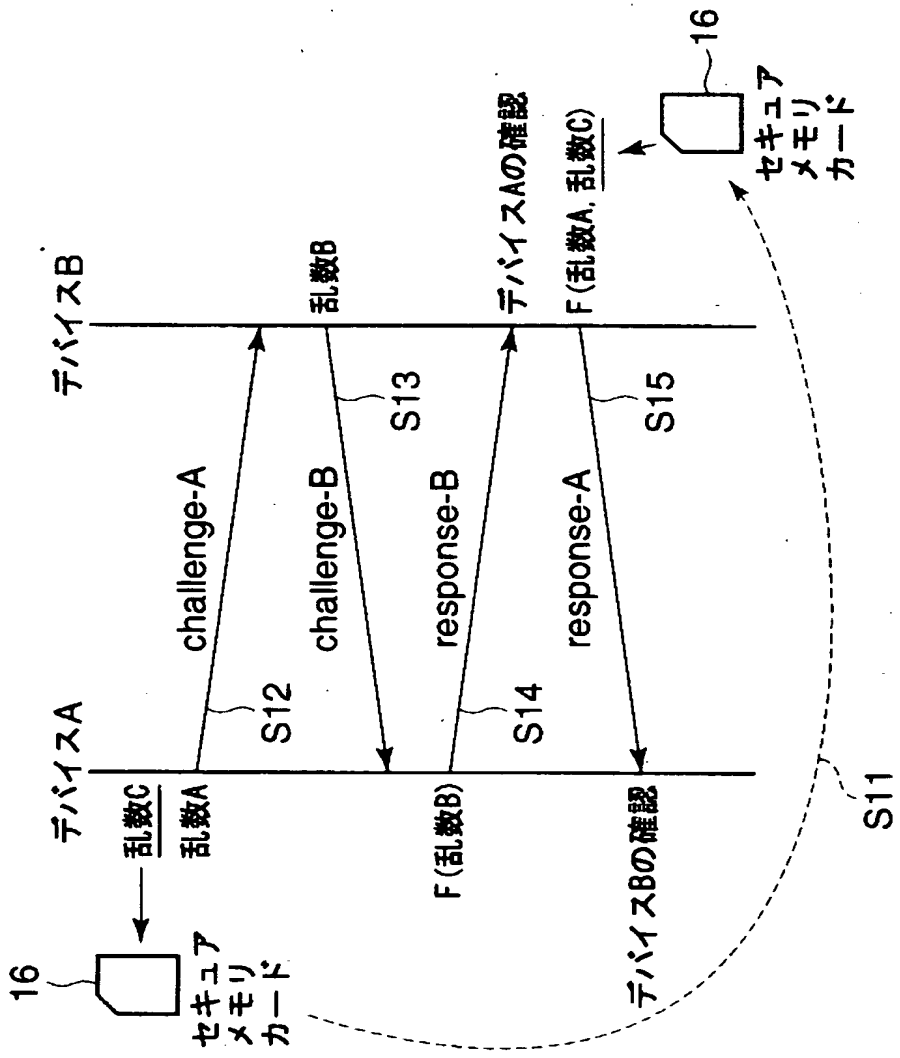
【図１】



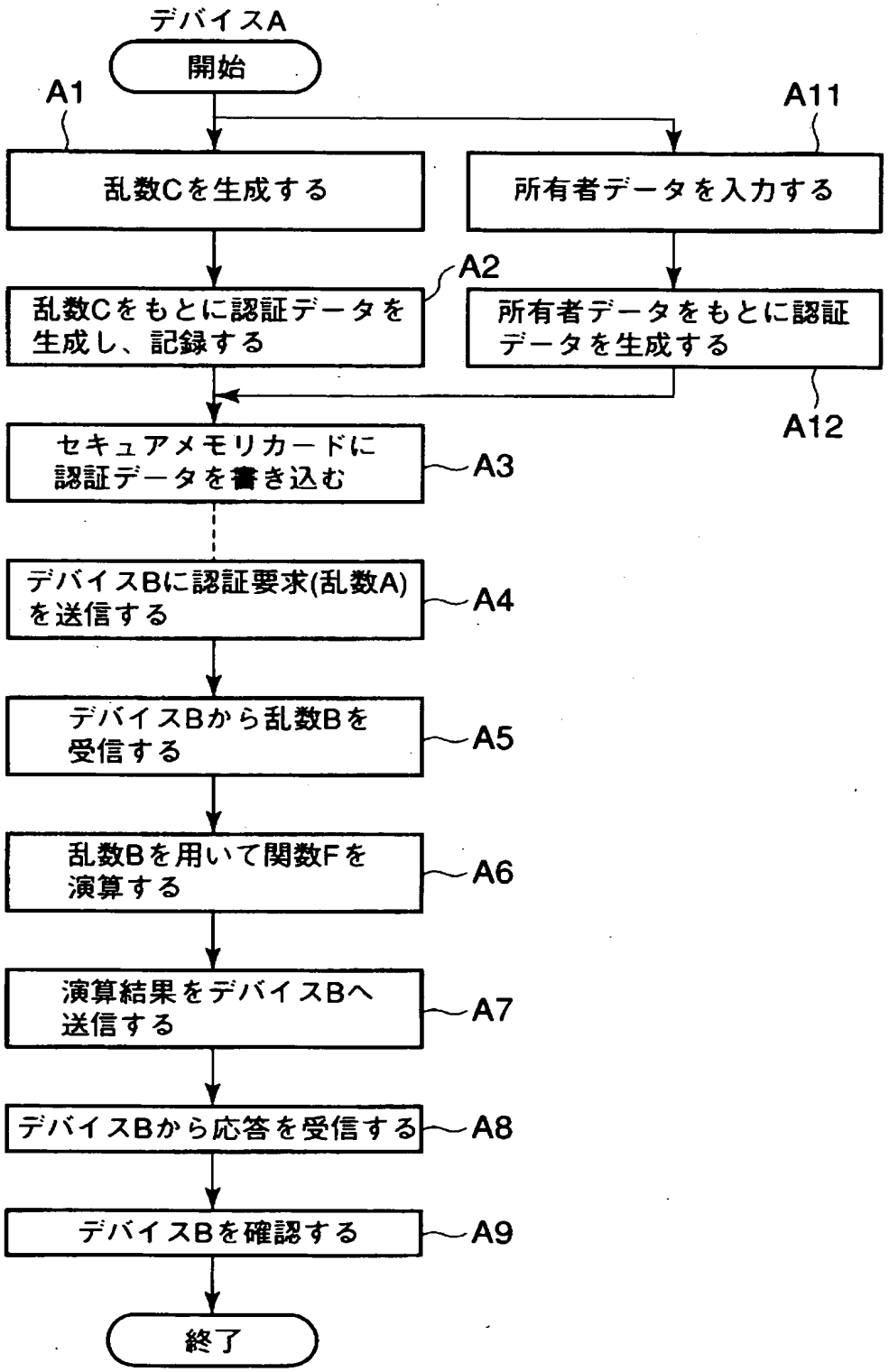
【図２】


12 デバイスB(クライアント)
10 デバイスA(サーバ)
CPU
ROM
認証プログラム
RAM
記憶装置
EEPROM
認証データ
乱数発生部
通信ユニット
カードスロット
生体情報入力装置
16 セキュアメモリカード
16 セキュアメモリカード
20
21
22
23
24
25
26
27
28
30
32

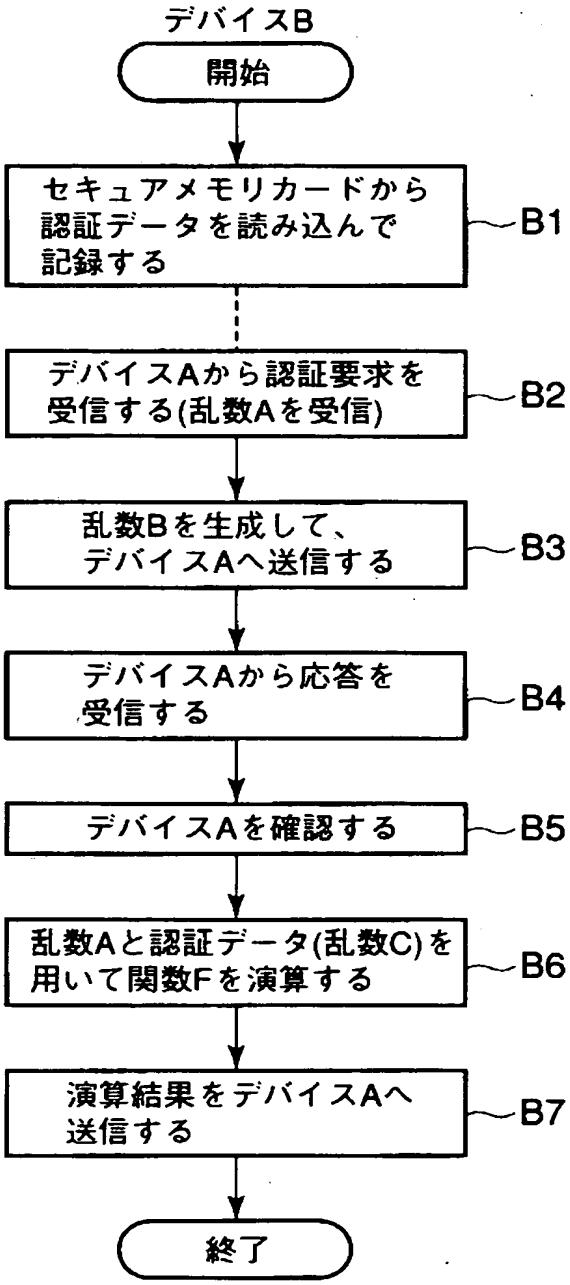
【図３】


16
セキュア
メモリ
カード
デバイスB
乱数B
デバイスAの確認
F(乱数A, 乱数C)
challenge-A
challenge-B
response-B
response-A
S12
S13
S14
S15
S11
デバイスA
乱数C
乱数A
F(乱数B)
デバイスBの確認
16
セキュア
メモリ
カード

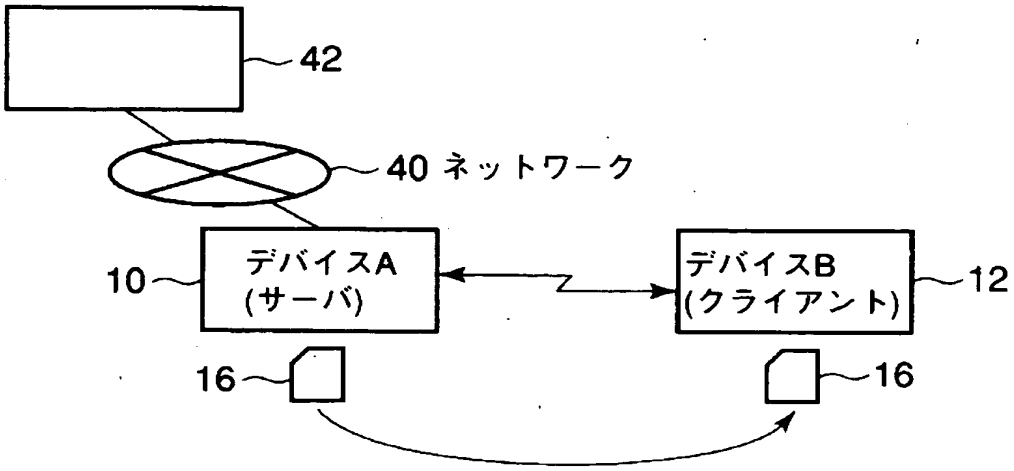
【図４】


デバイスA
開始
A1
A11
乱数Cを生成する
所有者データを入力する
A2
乱数Cをもとに認証データを生成し、記録する
所有者データをもとに認証データを生成する
A12
セキュアメモリカードに認証データを書き込む
A3
デバイスBに認証要求(乱数A)を送信する
A4
デバイスBから乱数Bを受信する
A5
乱数Bを用いて関数Fを演算する
A6
演算結果をデバイスBへ送信する
A7
デバイスBから応答を受信する
A8
デバイスBを確認する
A9
終了

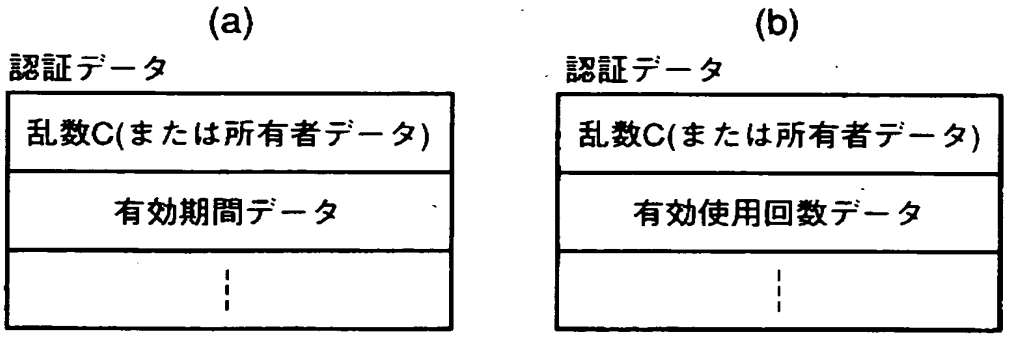
【図５】


デバイスB
開始
セキュアメモリカードから認証データを読み込んで記録する
B1
デバイスAから認証要求を受信する(乱数Aを受信)
B2
乱数Bを生成して、デバイスAへ送信する
B3
デバイスAから応答を受信する
B4
デバイスAを確認する
B5
乱数Aと認証データ(乱数C)を用いて関数Fを演算する
B6
演算結果をデバイスAへ送信する
B7
終了

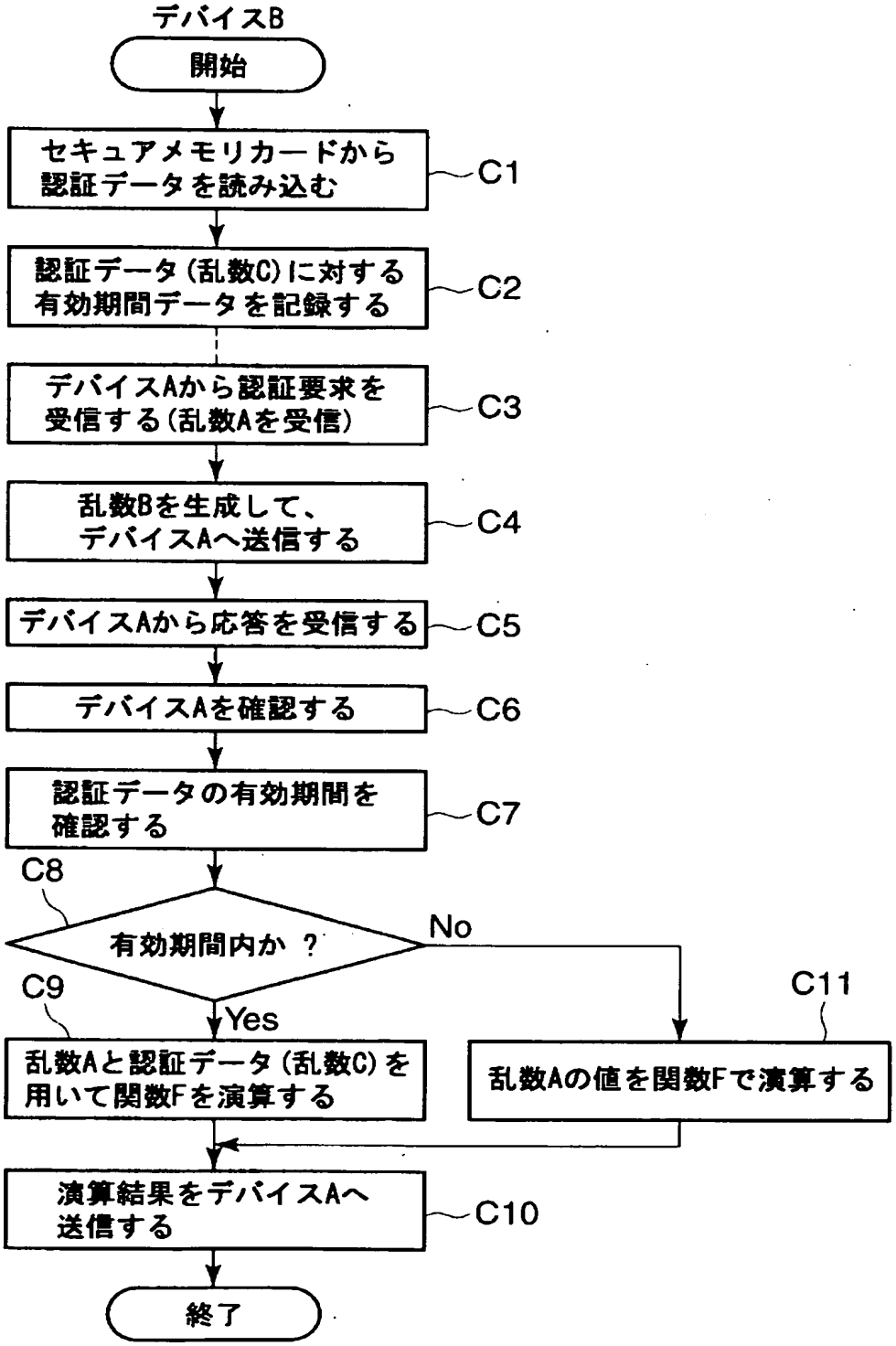
【図６】


42
40 ネットワーク
10
デバイスA
(サーバ)
デバイスB
(クライアント)
12
16
16

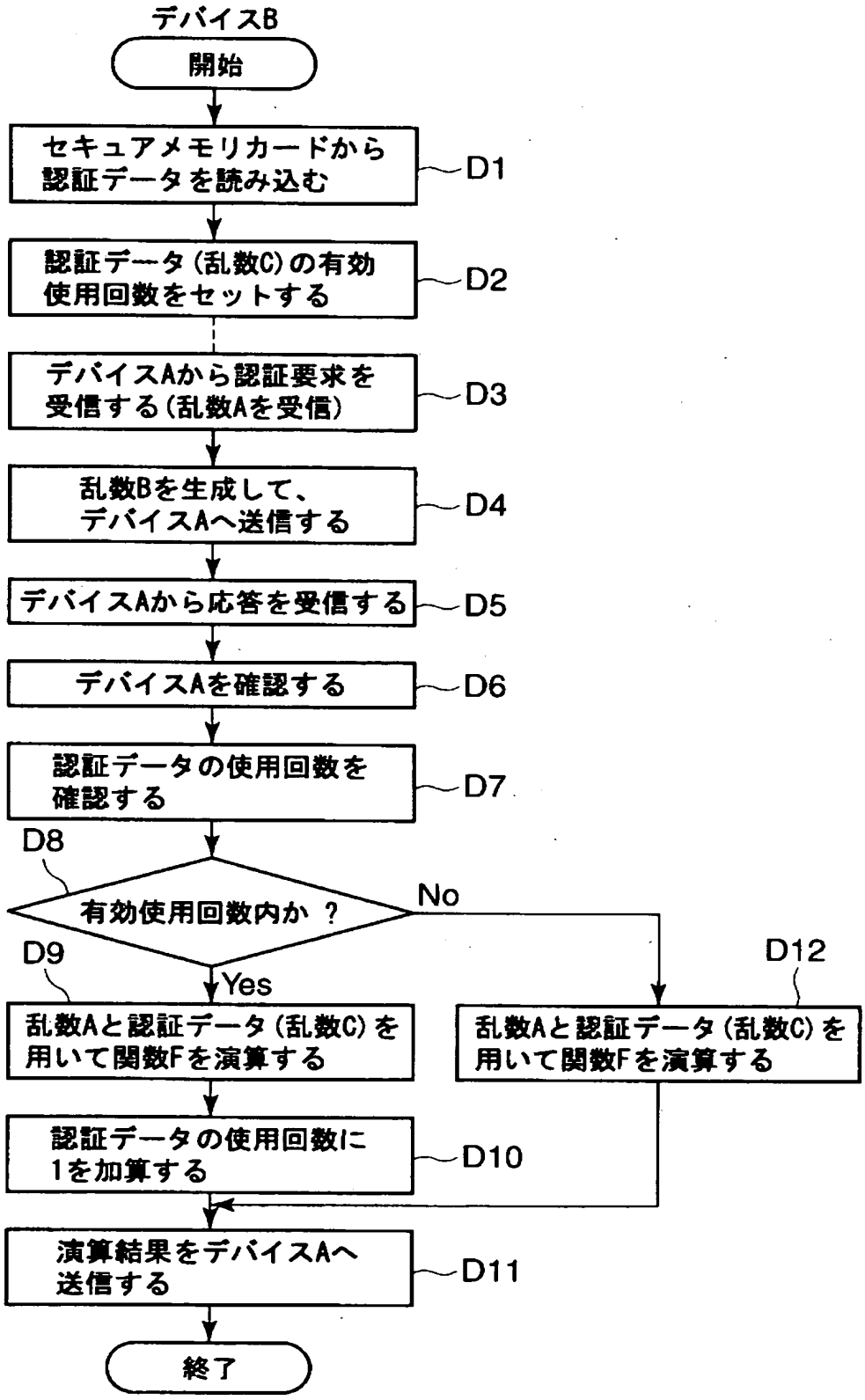
【図７】


(a)
認証データ
乱数C(または所有者データ)
有効期間データ
(b)
認証データ
乱数C(または所有者データ)
有効使用回数データ

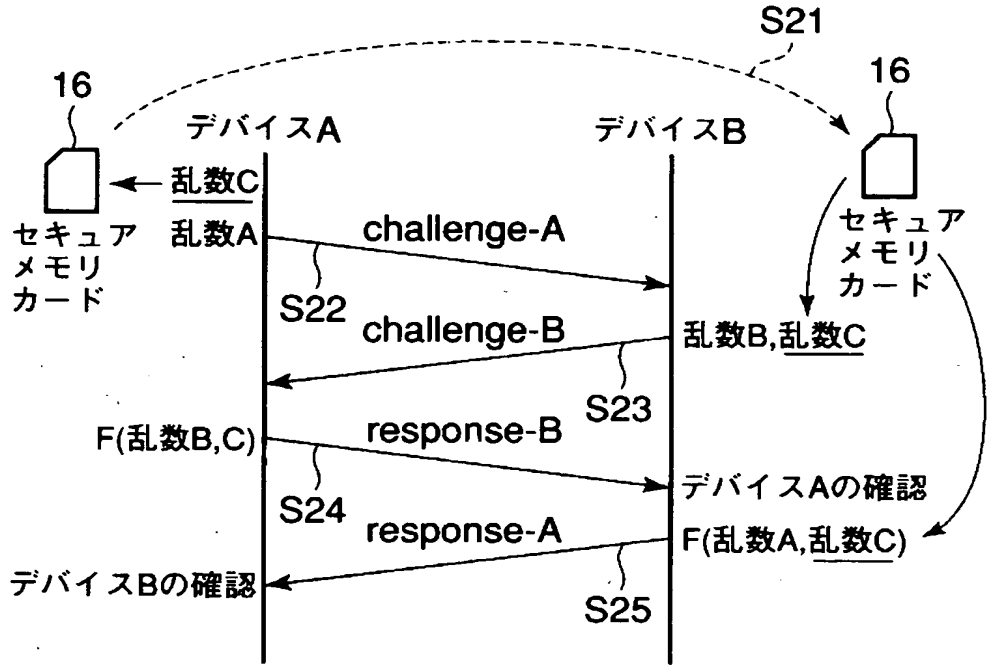
【図８】


デバイスB
開始
セキュアメモリカードから認証データを読み込む
C1
認証データ(乱数C)に対する有効期間データを記録する
C2
デバイスAから認証要求を受信する(乱数Aを受信)
C3
乱数Bを生成して、デバイスAへ送信する
C4
デバイスAから応答を受信する
C5
デバイスAを確認する
C6
認証データの有効期間を確認する
C7
C8
有効期間内か ?
No
Yes
C9
C11
乱数Aと認証データ(乱数C)を用いて関数Fを演算する
乱数Aの値を関数Fで演算する
演算結果をデバイスAへ送信する
C10
終了

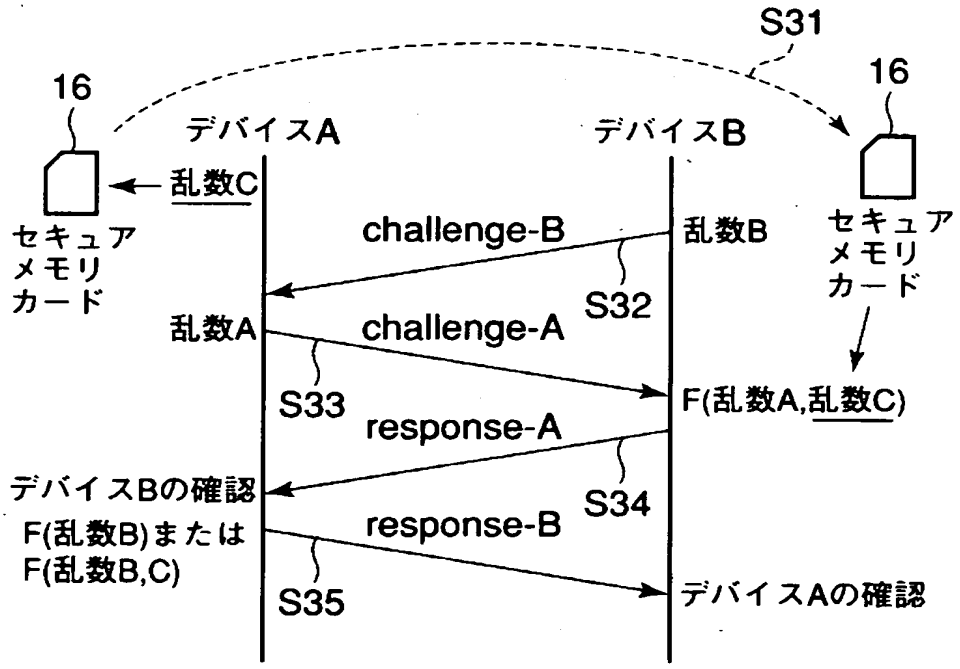
【図９】


デバイスB
開始
セキュアメモリカードから認証データを読み込む
D1
認証データ(乱数C)の有効使用回数をセットする
D2
デバイスAから認証要求を受信する(乱数Aを受信)
D3
乱数Bを生成して、デバイスAへ送信する
D4
デバイスAから応答を受信する
D5
デバイスAを確認する
D6
認証データの使用回数を確認する
D7
D8
有効使用回数内か ？
No
Yes
D9
D12
乱数Aと認証データ(乱数C)を用いて関数Fを演算する
乱数Aと認証データ(乱数C)を用いて関数Fを演算する
認証データの使用回数に1を加算する
D10
演算結果をデバイスAへ送信する
D11
終了

【図１０】


S21
16
16
デバイスA
デバイスB
乱数C
セキュア
メモリ
カード
乱数A
challenge-A
セキュア
メモリ
カード
S22
challenge-B
乱数B,乱数C
S23
F(乱数B,C)
response-B
デバイスAの確認
S24
response-A
F(乱数A,乱数C)
デバイスBの確認
S25

【図１１】


S31
16
16
デバイスA
デバイスB
乱数C
セキュア
メモリ
カード
challenge-B
乱数B
セキュア
メモリ
カード
S32
乱数A
challenge-A
S33
F(乱数A,乱数C)
response-A
デバイスBの確認
S34
F(乱数B)または
F(乱数B,C)
response-B
S35
デバイスAの確認

【書類名】　　要約書

【要約】

【課題】ライセンスされた正しい機器のうち、事前に認証機器側からオフラインで認証データを取得した被認証機器だけを接続可能にする。

【解決手段】認証時に使用される認証データを可搬型の記憶媒体（セキュアメモリカード１６）を通してオフラインで認証機器（デバイスＡ１０）側から被認証機器（デバイスＢ１２）側へ相互認証処理が行なわれる前に渡す。その後、デバイスＡ１０とデバイスＢ１２は、セキュアメモリカード１６を介して受け渡しされた認証データを用いて相互認証処理を実行する。

【選択図】　　図２

特願２００３－０９５６７１

出　願　人　履　歴　情　報

識別番号　　［０００００３０７８］

１．変更年月日　　２００１年　７月　２日
［変更理由］　　住所変更
住　所　　東京都港区芝浦一丁目１番１号
氏　名　　株式会社東芝

２．変更年月日　　２００３年　５月　９日
［変更理由］　　名称変更
住所変更
住　所　　東京都港区芝浦一丁目１番１号
氏　名　　株式会社東芝